

(12) NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES
PATENTWESENS (PCT) VERÖFFENTLICHTE INTERNATIONALE ANMELDUNG

(19) Weltorganisation für geistiges Eigentum
Internationales Büro



(43) Internationales Veröffentlichungsdatum
9. Januar 2003 (09.01.2003)

PCT

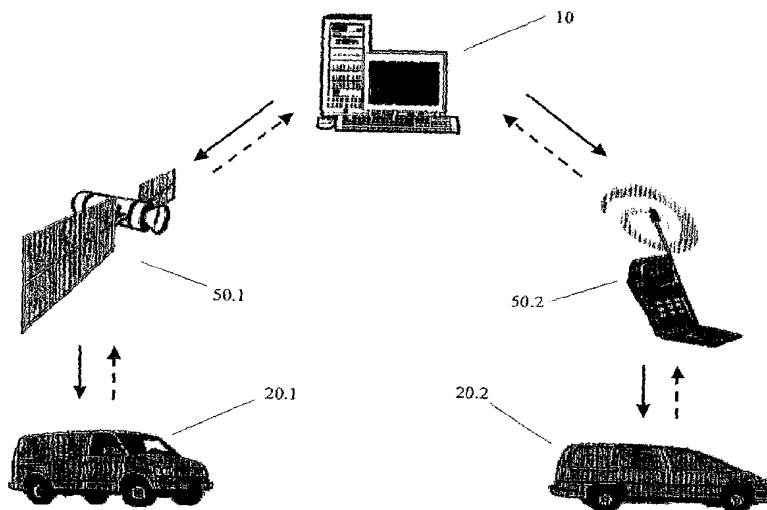
(10) Internationale Veröffentlichungsnummer
WO 03/003200 A1

- (51) Internationale Patentklassifikation⁷: **G06F 9/445**,
H04Q 7/32
- (21) Internationales Aktenzeichen: PCT/EP02/06994
- (22) Internationales Anmeldedatum:
25. Juni 2002 (25.06.2002)
- (25) Einreichungssprache: Deutsch
- (26) Veröffentlichungssprache: Deutsch
- (30) Angaben zur Priorität:
101 31 395.0 28. Juni 2001 (28.06.2001) DE
- (71) Anmelder (für alle Bestimmungsstaaten mit Ausnahme von
US): **DAIMLERCHRYSLER AG** [DE/DE]; Epplestrasse
225, 70567 Stuttgart (DE).
- (72) Erfinder; und
(75) Erfinder/Anmelder (nur für US): **DUERSCHMIDT, Ferry** [DE/DE]; Lehenstrasse 31/1, 71292 Friolzheim (DE). **KRAUTH, Andrej** [DE/DE]; Staufenstrasse 11/1, 73770 Denkendorf (DE). **MUELLER, Michael** [DE/DE]; Kronblumenweg 38, 70374 Stuttgart (DE).
- (74) Anwälte: **LINDNER-VOGT, Karin** usw.; Daimler-Chrysler AG, Intellectual Property Management, IPM-C106, 70546 Stuttgart (DE).
- (81) Bestimmungsstaaten (national): JP, US.
- (84) Bestimmungsstaaten (regional): europäisches Patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR).
- Veröffentlicht:
— mit internationalem Recherchenbericht

[Fortsetzung auf der nächsten Seite]

(54) Title: METHOD FOR TRANSMITTING SOFTWARE MODULES

(54) Bezeichnung: VERFAHREN ZUM ÜBERTRAGEN VON SOFTWARE-MODULEN



(57) Abstract: The invention relates to a method for transmitting software modules from a central unit to a mobile device, especially to a means of transport. To achieve this, a bi-directional wireless data transmission device is used and a set of software modules is selected. The configuration of the mobile device, which is actually available as transmission begins, is transmitted to the central unit. It is then necessary to check which software modules are released for the actually available configuration. Appliance-type identifications for the target appliances and software-type identifications for the software modules are used in release definitions which are applied in a release test. The software modules which are selected and released for the actually available configuration are transmitted. Said method can be used in the same way for supplying a single mobile device or families of mobile devices which are rich or deficient in variants.

[Fortsetzung auf der nächsten Seite]



WO 03/003200 A1



- vor Ablauf der für Änderungen der Ansprüche geltenden Frist; Veröffentlichung wird wiederholt, falls Änderungen eintreffen
- Zur Erklärung der Zweibuchstaben-Codes und der anderen Abkürzungen wird auf die Erklärungen ("Guidance Notes on Codes and Abbreviations") am Anfang jeder regulären Ausgabe der PCT-Gazette verwiesen.

(57) Zusammenfassung: Die Erfindung betrifft ein Verfahren zum Übertragen von Software-Modulen von einer Zentrale zu einer mobilen Vorrichtung, insbesondere zu einem Verkehrs- oder Transportmittel. Für die Übertragung wird eine Einrichtung zur drahtlosen Datenübertragung in beiden Richtungen verwendet, und eine Menge von Software-Modulen wird ausgewählt. Die zu Beginn der Übertragung tatsächlich vorhandene Konfiguration der mobilen Vorrichtung wird an die Zentrale übermittelt. Geprüft wird, welche dieser Software-Module für die tatsächlich vorhandene Konfiguration freigegeben sind. Dabei werden für die Ziel-Geräte Geräte-Typ-Kennungen und für die Software-Module Software-Typ-Kennungen in Freigabe-Festlegungen verwendet. Diese Freigabe-Festlegungen werden bei einer Freigabe-Prüfung verwendet. Die ausgewählten und für die tatsächlich vorhandene Konfiguration freigegebenen Software-Module werden übertragen. Das Verfahren ist in gleicher Weise für die Versorgung einer einzelnen mobilen Vorrichtung wie auch für Familien von variantenreichen oder variantenarmen mobilen Vorrichtungen anwendbar.

Verfahren zum Übertragen von Software-Modulen

Die Erfindung betrifft ein Verfahren zum Übertragen von Software-Modulen von einer Zentrale zu einer Ziel-Vorrichtung mit Hilfe einer Einrichtung zur Datenübertragung in beiden Richtungen. Die Ziel-Vorrichtung ist eine mobile Vorrichtung, vorzugsweise ein Verkehrs- oder Transportmittel.

In mobilen Vorrichtungen, insbesondere in Kraftfahrzeugen, wird eine steigende Anzahl von Geräten verwendet, die durch Software-Module gesteuert werden, z. B. Tür-Steuergeräte. Manche Geräte, z. B. elektronische Navigationssysteme und Systeme zur Sprachausgabe, benötigen umfangreiche Datenbibliotheken. Um mobile Vorrichtungen an individuelle Anforderungen und Wünsche von Benutzern oder Betreibern anzupassen, werden oft Ziel-Geräte in vielen unterschiedlichen Versionen und Varianten hergestellt und eingebaut, manchmal auch nachträglich. Durch die Kombination von Varianten entsteht eine hohe Zahl unterschiedlicher Konfigurationen von Ziel-Geräten an Bord von mobilen Vorrichtungen, die zu einer Familie von mobilen Vorrichtungen gehören. Der Hersteller einer mobilen Vorrichtung hat trotz der Variantenvielfalt zu gewährleisten, dass diese Ziel-Geräte in jeder freigegebenen Kombination im laufenden Betrieb sicher zusammenspielen.

Mit „Software-Module“ werden insbesondere Programme oder Teile von Programmen, die an Bord von mobilen Vorrichtungen ausgeführt werden, und Daten für solche Programme oder für Ziel-Geräte sowie Parameter von Ziel-Geräten bezeichnet. Mit „Ziel-Geräten“ werden diejenigen datenverarbeitenden Geräte an Bord einer mobilen Vorrichtung bezeichnet, für die Software-Module zu übertragen sind, hierzu zählen insbesondere Steuergeräte z. B. für Türen oder die Klimaanlage. Ein zu

übertragender Parameter beeinflusst beispielsweise die Funktionsweise eines Ziel-Geräts oder aktiviert oder deaktiviert ein Programm an Bord der mobilen Vorrichtung.

Es ist heute noch üblich, zum nachträglichen Übertragen von Software-Modulen in mobile Vorrichtungen die Ziel-Geräte z. B. in einer Werkstatt auszubauen, mit den gewünschten Software-Modulen zu versehen und dann wieder einzubauen. In manchen Fällen muß das Ziel-Gerät sogar zum Hersteller geschickt werden, der zentral die Software-Module überträgt. Diese Wege sind teuer und zeitaufwendig.

Ein Verfahren nach dem Oberbegriff des Anspruchs 1 ist aus DE 68920462 T2 bekannt. Die Aufgabe von DE 68920462 T2 ist eine On-line-Problemlösung in einem Kundensystem durch ein zentrales Fernwartungssystem.

Eine Problemverwaltungs-Datenbank erhält Serviceanforderungen als Suchargumente und liefert Lösungsansätze für die Fehlerbeseitigung. Sie enthält Einträge, die eine Vielzahl von Komponenten und Symptome als Suchargumente und Problemlösungen als Ausgabedaten miteinander verbinden. Vorzugsweise besteht die Problemverwaltungs-Datenbank aus drei getrennten Einheiten, nämlich eine Symptomausnahmetabelle mit Einträgen für Hardware-Komponenten, eine APAR-Tabelle für Software-Komponenten mit vorläufigen Programmkorrekturen und eine MTAR-Tabelle mit Korrekturen für Microcode. Die Suchargumente sind vorzugsweise Symptomfolgen, die als Referenzschlüssel formatiert sind, welche austauschbare Komponenten („field replaceable units“, FRUs) kennzeichnen, und die Nummer und den Austrittspunkt eines Problemlösungsverfahrens kennzeichnen. Beispielsweise besteht die Symptomfolge aus den beiden wahrscheinlichsten Fehlern.

Die Problemverwaltungs-Datenbank von DE 68920462 T2 benötigt als Suchargumente entdeckte Symptome und Austrittspunkte von Problembestimmungsverfahren. Eine Serviceanforderung kennzeichnet ein bestimmtes Kundensystem und Ergebnisse des Problembestimmungsverfahrens. Die Problemverwaltungs-Datenbank ist so aufgebaut, dass ihre Ausgabedaten die Problemlösung festlegen.

Die Problemverwaltungs-Datenbank ist notwendigerweise komplex, und ihre Auswertung benötigt einige Rechenzeit. Denn in der Regel kann ein Bauteil durch unterschiedliche Fehler gestört sein, und ein Fehler an einem Bauteil kann Fehler an anderen Bauteilen hervorrufen. Daher sind meist wesentlich mehr Symptome zu berücksichtigen, als Bauteile vorhanden sind.

Vor der Übertragung von Software-Modulen wird in DE 68920462 T2 auf Konfigurationsdaten der Ziel-Vorrichtung zugegriffen. Die Konfiguration der Hardware- und Software-Komponenten zum Zeitpunkt der Störung wird dadurch erfaßt. Diese Konfigurationsdaten werden von einem Ressourcen-Manager-System vorzugsweise in einer Tabelle verwaltet. Für mobile Vorrichtungen ist es - z. B. wegen knapper Speicherkapazität an Bord - oft nicht oder nur mit Aufwand möglich, eine solche Tabelle an Bord zu führen und aktuell zu halten. Insbesondere im Falle mobiler Vorrichtungen besteht darüber hinaus die Gefahr, dass die Tabelle mit der Konfiguration nicht mit der tatsächlichen Konfiguration der Ziel-Vorrichtung übereinstimmt, weil ein Benutzer oder Betreiber der mobilen Vorrichtung ein Ziel-Gerät austauscht oder ergänzt. Ein solcher Betreiber oder Benutzer ist in der Regel kein DV-Fachmann, sondern z. B. ein Autofahrer. Daher darf nicht davon ausgegangen werden, dass eine Konfigurations-Tabelle stets die aktuelle Konfiguration der mobilen Vorrichtung enthält.

Aus DE 19750372 A1 ist ein Verfahren zum Übertragen von Programmen und / oder Daten von einem zentralen Server an ein Fahrzeug bekannt. Die Übertragung erfolgt per Funkverbindung. Fahrzeug und Server haben je ein Sende- und Empfangsgerät. Geprüft wird, ob der Benutzer eine Zugriffsberechtigung für die angeforderten Programme und/oder Daten besitzt. Für diese Prüfung werden Daten vom Fahrzeug an die Zentrale gemeldet.

In DE 19750372 A1 wird keine Lösung für die Probleme offenbart, dass viele Varianten der mobilen Vorrichtung im Einsatz sein können und dass Ziel-Geräte an Bord einer mobilen Vorrichtung sich gegenseitig beeinflussen können.

In DE 19853000 A1 wird ein Verfahren zum Versorgen von Kraftfahrzeugen mit Daten sowie zum Austausch, Abfragen, Ändern, Aktualisieren von Daten offenbart. Verwendet wird eine drahtlose Datenübertragungseinrichtung. Die Daten sind vorzugsweise Überwachungsdaten, z. B. Betriebsdaten von Bremsen, Fahrwerk, Ölstand, oder sie sind Programme oder Programmteile.

Aus DE 19532067 C1 ist ein Verfahren zum Einprogrammieren von Daten in ein Fahrzeug-Bauteil bekannt. Daten werden von einer Zentrale an die anfordernde Stelle übertragen. Insbesondere um unberechtigten Zugriff auf die übertragenen Daten zuverlässig zu unterbinden, werden Informationen zur Identität von Fahrzeug, Bauteil und Nutzer an die Zentrale übermittelt.

Aus DE 19921845 A1 ist eine Diagnosetestvorrichtung für Kraftfahrzeuge mit programmierbaren Steuergeräten bekannt. Ein externer Diagnosetester ist mit einer Programmerkennungs- und Programmladevorrichtung ausgestattet. Bei Bedarf wird die jeweils aktuellste Version eines Programms in den Programmspeicher des entsprechenden Steuergeräts geladen.

Die oben genannten Druckschriften offenbaren Verfahren, um Software-Module an eine mobile Vorrichtung zu übermitteln und dabei bei Bedarf Berechtigungs- und Freigabeprüfungen durchzuführen. Die Prüfungen beziehen sich jeweils auf eine einzelne mobile Vorrichtung. Jedoch wird bei den Verfahren die Möglichkeit nicht berücksichtigt, dass Software-Module an variantenreiche mobile Vorrichtungen zu übertragen sind. Der Variantenreichtum wird auch nicht dadurch berücksichtigt, dass - wie in DE 19853000 A1 - Überwachungsdaten vom Fahrzeug an die Zentrale übermittelt werden. Der Variantenreichtum resultiert beispielsweise daher, dass in verschiedenen Exemplaren einer Familie von mobilen Vorrichtungen, z. B. einer Fahrzeugflotte, unterschiedliche Ziel-Geräte eingebaut sind oder dass Ziel-Geräte in unterschiedlichen Versionen und Varianten verwendet werden oder verschiedene Software-Module aktiviert worden sind. Der Variantenreichtum kann zu einer riesigen Zahl unterschiedlicher Prüfungen führen, die nicht mit vertretbarem Aufwand definiert und validiert werden können.

Weiterhin wird nicht die Möglichkeit berücksichtigt, dass ein Benutzer oder Betreiber einer mobilen Vorrichtung ein Ziel-Gerät erneuert oder nachträglich ergänzt, ohne dass der Hersteller der mobilen Vorrichtung hierüber informiert wird und dies bei einer Freigabe-Prüfung nach dem Stand der Technik berücksichtigen kann. Auch beim Verfahren nach DE 19532067 C1, bei dem Informationen über die Fahrzeug-Identität an die Zentrale übermittelt werden, wird die Möglichkeit nachträglicher Änderungen nicht berücksichtigt. Zwar kann die Zentrale sich eine abgespeicherte Konfigurations-Datei des Fahrzeugs beschaffen, diese Informationen können aber falsch oder veraltet sein.

Variantenreichtum und nachträgliche Änderungen sind aber zu berücksichtigen, um sicherzustellen, dass zu jeder mobilen Vorrichtung die richtigen Software-Module übertragen werden und sichergestellt wird, dass die übertragenen Software-Module auf dem Fahrzeug fehlerfrei miteinander und mit den Ziel-Geräten an Bord zusammenspielen und nicht zu unerwünschten oder fehlerhaften Betriebszuständen führen.

Ausgehend von DE 68920462 T2 liegt der Erfindung die Aufgabe zugrunde, ein Verfahren nach dem Oberbegriff von Anspruch 1 zu schaffen, das auch dann gewährleistet, dass nur die richtigen und keine anderen Software-Module übertragen werden, wenn variantenreiche Familien von Ziel-Vorrichtungen mit Ziel-Geräten verschiedener Hersteller vorliegen oder wenn die Möglichkeit nachträglicher Änderungen an einzelnen Ziel-Vorrichtungen, über welche die Zentrale nicht informiert ist, zu berücksichtigen ist. Weiterhin ist eine Übertragungs-Vorrichtung zur Durchführung des Verfahrens bereitzustellen.

Die Aufgabe wird durch ein Verfahren nach Anspruch 1 und eine Übertragungs-Vorrichtung nach Anspruch 10 gelöst. Vorteilhafte Ausgestaltungen sind in den Unteransprüchen angegeben.

Für die Übertragung wird eine Einrichtung zur drahtlosen Datenübertragung in beiden Richtungen verwendet, und eine Menge von Software-Modulen wird ausgewählt. Diese Menge besteht aus mehreren Software-Modulen oder aus nur einem einzigen Software-Modul. Informationen über die aktuelle Konfiguration der

mobilen Vorrichtung werden an die Zentrale übermittelt. Mit „aktueller Konfiguration“ wird die tatsächliche zu Beginn der Übertragung vorhandene Konfiguration bezeichnet. Diese Informationen umfassen eine Auflistung, welche Ziel-Geräte und welche Software-Module zu Beginn der Übertragung an Bord der mobilen Vorrichtung tatsächlich vorhanden sind. Geprüft wird, welche dieser Software-Module für die aktuelle Konfiguration freigegeben sind. Die ausgewählten und für die aktuelle Konfiguration freigegebenen Software-Module werden übertragen.

Für eine Freigabe-Prüfung werden Freigabe-Festlegungen verwendet, die wie folgt erzeugt werden: Für die Ziel-Geräte werden Geräte-Typ-Kennungen festgelegt, also Kennungen für die Typen von Ziel-Geräten. Für die Software-Module werden Software-Typ-Kennungen festgelegt. Unter Verwendung der Geräte-Typ-Kennungen und Software-Typ-Kennungen wird festgelegt, welche der ausgewählten Software-Module für welche Typen von Ziel-Geräten freigegeben sind. Diese Freigabe-Festlegungen werden verwendet, um zu entscheiden, welche Software-Module für die zu Beginn der Übertragung tatsächlich vorhandene Konfiguration freigegeben sind.

Das Verfahren ist in gleicher Weise für die Versorgung einer einzelnen mobilen Vorrichtung wie auch für Familien von variantenreichen oder variantenarmen mobilen Vorrichtungen anwendbar. Insbesondere werden auch dann zuverlässig die richtigen und keine anderen Software-Module ausgewählt und übertragen, wenn in der mobilen Vorrichtung mehrere Ziel-Geräte unterschiedlicher Hersteller vorhanden sind und diese Ziel-Geräte in unterschiedlichen Versionen und Varianten vorkommen, die unterschiedliche Software-Module benötigen.

Die richtigen Software-Module werden auch dann ausgewählt und übertragen, wenn ein Benutzer oder Betreiber der mobilen Vorrichtung ein Ziel-Gerät durch ein andersartiges ersetzt hat oder nachträglich ein weiteres Ziel-Gerät ergänzt hat. Dies wird insbesondere dadurch erreicht, dass ermittelt wird, welche Ziel-Geräte und Software-Module sich zum Zeitpunkt der Übertragung tatsächlich in der mobilen Vorrichtung befinden. Nicht mehr erforderlich ist es, eine Abfrage in einer zentra-

len Datenbank mit Konfigurationen von mobilen Vorrichtungen durchzuführen. Die Einträge in einer solchen zentralen Datenbank können veraltet sein, z. B. weil ein Ziel-Gerät durch ein andersartiges ersetzt wurde oder ein Ziel-Gerät ergänzt oder entfernt wurde, ohne dass der Hersteller hierüber informiert wurde.

Dank der Verwendung einer drahtlosen Datenübertragungseinrichtung ist es nicht erforderlich, dass die mobile Vorrichtung zum Übertragen in eine Werkstatt gefahren oder transportiert wird. Es ist möglich, ein Software-Modul bereits unmittelbar nach seiner Fertigstellung und / oder Freigabe zu übertragen.

Einige beispielhafte Anwendungen, in denen das erfindungsgemäße Verfahren Vorteile gegenüber dem Stand der Technik erbringt, sind die folgenden:

- Auf Initiative des Kundendienstes eines Fahrzeugherstellers wird eine Kundendienstmaßnahme für alle Fahrzeuge eines Typs durchgeführt. Beispielsweise wird für alle Fahrzeuge einer Baureihe und eines Baujahrs eine neue Version eines Software-Moduls übertragen. Oder eine gesetzliche Bestimmung in einem Staat wird geändert, und Software-Module werden an Fahrzeuge in diesem Staat übertragen, um den geänderten Gesetzen nachzukommen. Besitzer und Nutzer der mobilen Vorrichtung werden informiert, und die Software-Module werden bei Einverständnis erfindungsgemäß übertragen. Durch das erfindungsgemäße Verfahren ist es nicht erforderlich, dass ein Fahrzeug des Typs in eine Werkstatt gebracht wird, und es wird sichergestellt, dass die neue Version des Software-Moduls nur auf diejenigen Fahrzeuge übertragen wird, für deren Konfigurationen sie freigegeben ist.
- Für einen bestimmten Fahrzeugtyp sollen umfangreiche Betriebsdaten an Bord aufgezeichnet, vorverarbeitet und an eine Zentrale übermittelt werden. Ein Programm, das die Aufzeichnung, Vorverarbeitung und Übermittlung übernimmt und dabei die Daten gegen unbefugten Zugriff sichert, wird durch das erfindungsgemäße Verfahren übertragen, nachdem der Eigentümer hierzu sein Einverständnis gegeben hat.

Durch die Kenntnis der aktuellen Konfiguration wird sichergestellt, dass das übertragene Programm auf die tatsächlich an Bord vorhandenen Geräte zugeschnitten ist.

- Ein Besitzer einer mobilen Vorrichtung kauft vom Hersteller der mobilen Vorrichtung eine zusätzliche oder verbesserte Funktionalität, die ausschließlich durch zusätzliche Software-Module auf bereits eingebauten Ziel-Geräten realisiert wird. Durch das Verfahren wird es ermöglicht, dass die Software-Module ohne einen Werkstattbesuch übertragen werden, wenn eine drahtlose Verbindung hergestellt werden kann. Sichergestellt wird, dass die Software-Module für die mobile Vorrichtung freigegeben sind.
- Ein Ziel-Gerät an Bord eines Fahrzeugs ist ausgefallen, und das Fahrzeug kann seine Fahrt nicht fortsetzen. Ein Wartungstechniker fährt mit einem neuen Ziel-Gerät zum Fahrzeug. Das neue Gerät ist hinsichtlich der Hardware baugleich oder wenigstens funktionsgleich zum ausgefallenen Gerät, jedoch sind keine Software-Module in ihm abgespeichert. Die benötigten Software-Module werden durch das erfindungsgemäße Verfahren übertragen. Dadurch ist es nicht erforderlich, dass der Wartungstechniker die Software-Module sowie eine Einrichtung zur Konfigurations-Ermittlung und Freigabe-Prüfung mit sich führt. Da der Wartungstechniker für eine Flotte von unterschiedlichen Fahrzeugen mit verschiedenen Geräten an Bord verantwortlich ist, ist es wegen der Variantenvielfalt nicht möglich, dass er alle Software-Module mit sich führt, die beim Ausfall eines Ziel-Geräts an Bord eines der Fahrzeuge benötigt werden. Das erfindungsgemäße Verfahren spart erheblich Zeit gegenüber dem Vorgehen ein, dass der Wartungstechniker erst nach einem Ausfall eines Geräts ermittelt, welche Software-Module für das neue Gerät benötigt werden, und diese Software-Module dann von einer Zentrale beschafft.

Die Menge von Software-Modulen wird beispielsweise wie folgt ausgewählt (Anspruch 2): Die an die Zentrale übermittelte aktuelle Konfiguration der mobilen Vorrichtung wird mit einer Wunsch- oder Soll-Konfiguration verglichen. Eine Wunsch-

Konfiguration wird beispielsweise dadurch erzeugt, dass ein Eigentümer der mobilen Vorrichtung zusätzliche Funktionalitäten erwirbt, eine Soll-Konfiguration dadurch, dass der Hersteller der mobilen Vorrichtung vorsieht, dass alle mobilen Vorrichtungen einer Baureihe mit einem bestimmten Software-Modul versorgt werden. Die Software-Module werden in Abhängigkeit von der Abweichung zwischen aktueller und Wunsch- bzw. Soll-Konfiguration ausgewählt. Beispielsweise werden alle Software-Module ausgewählt, die in der Wunsch- bzw. Soll-Konfiguration auftreten, aber in der aktuellen Konfiguration gar nicht oder nur in einer älteren Version.

Anspruch 3 sieht vor, dass vor der Übertragung der Software-Module geprüft wird, ob mit Hilfe der drahtlosen Datenübertragungseinrichtung ein Übertragungskanal mit einer für die Übertragung ausreichenden Güte aufgebaut werden kann. Insbesondere wird geprüft, ob überhaupt eine Verbindung aufgebaut wird und ob diese Verbindung eine ausreichende Bandbreite besitzt. Bevorzugt werden die Software-Module vor der Übertragung komprimiert und nach der Übertragung dekomprimiert, um Übertragungszeit einzusparen.

Dank der Ausgestaltung nach Anspruch 4 kann das erfindungsgemäße Verfahren auch dann durchgeführt werden, wenn die aktuelle Konfiguration nicht komplett an die Zentrale übermittelt werden kann und daher benötigte Informationen fehlen, beispielsweise weil nicht alle Informationen über die aktuelle Konfiguration an Bord abgespeichert worden sind oder weil die Datenverbindung von der mobilen Vorrichtung zur Zentrale gestört ist. Hingegen haben diejenigen Informationen über die aktuelle Konfiguration, die an die Zentrale übermittelt wurden und nicht unzutreffend sind, Vorrang vor den abgespeicherten Konfigurations-Informationen.

Gemäß der Ausgestaltung nach Anspruch 4 werden Informationen über eine der Zentrale bekannte Konfiguration der mobilen Vorrichtung in einem Konfigurations-Management-System oder Dokumentations-System abgespeichert. Beispielsweise umfaßt das System eine Datenbank, in der ein Datensatz für die mobile Vorrichtung bei ihrer Fertigstellung angelegt wird. Wäh-

rend der Übertragung wird eine Kennung der mobilen Vorrichtung zur Zentrale übermittelt. Diese Kennung unterscheidet diese mobile Vorrichtung wenigstens von allen anderen mobilen Vorrichtungen desselben Herstellers. Die an die Zentrale übermittelten Informationen über die aktuelle Konfiguration werden mit den abgespeicherten Informationen über die Konfiguration verglichen.

Nachdem die Kennung der mobilen Vorrichtung an die Zentrale übermittelt wurde, wird auf den Datensatz für diese mobile Vorrichtung zugegriffen. Nicht übermittelte Informationen über die aktuelle Konfiguration werden durch Lesezugriff auf die abgespeicherte Konfiguration ergänzt. Auf die abgespeicherte Konfiguration wird insbesondere dann zugegriffen, wenn die aktuelle Konfiguration nur unvollständig an die Zentrale übermittelt wird und daher benötigte Informationen über die aktuelle Konfiguration, beispielsweise der Typ eines tatsächlich zum Zeitpunkt der Übertragung eingebauten Tür-Steuergerätes, fehlen. Bevorzugt werden die an die Zentrale übermittelten Informationen über die aktuelle Konfiguration einer Plausibilitätsprüfung unterzogen, um insbesondere Übertragungsfehler zu erkennen. Werden hierbei einzelne Informationen als offensichtlich unzutreffend erkannt, so werden die unzutreffenden der übermittelten Informationen durch die entsprechenden abgespeicherten Informationen ersetzt.

Bevorzugt werden die Software-Module nach der Übertragung zunächst in einem Pufferspeicher an Bord der mobilen Vorrichtung abgespeichert. Sie werden dann an die jeweiligen Ziel-Geräte verteilt und zu diesen übertragen. Vorzugsweise werden daher gemeinsam mit den Software-Modulen Meta-Informationen übertragen, die die Verteilung und / oder Übertragung und / oder Aktivierung der Software-Module an Bord der mobilen Vorrichtung steuern.

Die drahtlose Datenverbindung zwischen Zentrale und mobiler Vorrichtung kann gestört sein, weswegen die Übertragung der Software-Module nicht fehlerfrei abgeschlossen werden kann. Oft ist der Hersteller von mobilen Vorrichtungen gesetzlich verpflichtet, zu dokumentieren, welche Software-Module sich

an Bord der von ihm hergestellten mobilen Vorrichtungen befinden. Beispielsweise aus diesen beiden Gründen wird nach der Übertragung mindestens eines der Software-Module die Information an die Zentrale übermittelt, ob das Software-Modul tatsächlich fehlerfrei an die mobile Vorrichtung übermittelt wurde (Anspruch 5). Bevorzugt wird nach jeder Übertragung eines Software-Moduls eine Information über das Ergebnis der Übertragung an die Zentrale übermittelt. Falls bei der Übertragung Fehler auftraten, wird bevorzugt zusätzlich eine Fehlerbeschreibung an die Zentrale übermittelt.

Durch die erfolgreiche Übertragung von Software-Modulen wird die aktuelle Konfiguration der mobilen Vorrichtung verändert. Insbesondere um gesetzlichen Auflagen nach einer Produktdokumentation nachzukommen, wird gemäß Anspruch 6 eine Rückdokumentation durchgeführt. Hierfür wird die Kennung der mobilen Vorrichtung zur Zentrale übermittelt. Diese Kennung unterscheidet diese mobile Vorrichtung wenigstens von allen anderen mobilen Vorrichtungen desselben Herstellers. In einem Konfigurations-Management-System wird die Information abgespeichert, welche Ziel-Geräte-Typen und welche Software-Module nach Abschluß der Übertragung an Bord der mobilen Vorrichtung tatsächlich vorhanden sind. Informationen über die Ziel-Geräte-Typen wurden erfindungsgemäß bereits für die Freigabe-Prüfungen an die Zentrale übermittelt.

Die Information, welche Software-Module fehlerfrei und unverfälscht übertragen wurden, wird auch für eine Synchronisation nach einem Fehlerfall, z. B. nach einem Verbindungsabbruch, verwendet. Ermittelt wird, welche Software-Module bei einem zweiten Versuch für die Übertragung vorgesehen werden.

Die übertragenen Software-Module werden bevorzugt nur dann aktiviert, wenn die mobile Vorrichtung sich in einem sicheren Zustand befindet. Ansonsten besteht die Gefahr, dass während der Aktivierung eines Software-Moduls oder der dafür erforderlichen Deaktivierung eines zuvor vorhandenen Software-Moduls die mobile Vorrichtung in einen unerwünschten Betriebszustand gerät. Beispielsweise ist sicherzustellen, dass Software-Module für Steuergeräte an Bord eines Kraftfahrzeu-

ges nur bei stehendem Fahrzeug aktiviert werden. Anspruch 7 sieht vor, dass zusätzlich Informationen über den aktuellen Betriebszustand der mobilen Vorrichtung an die Zentrale übermittelt werden. In Abhängigkeit von den Betriebszustands-Informationen wird entschieden, ob die mobile Vorrichtung sich in einem sicheren Zustand befindet. Dann, wenn sie sich in einem sicheren Zustand befindet, werden die übertragenen Software-Module aktiviert.

Die Übertragung kann sowohl von der Zentrale als auch von einer Stelle außerhalb der Zentrale, beispielsweise einem Eigentümer, Fahrer oder Nutzer der mobilen Vorrichtung, angefordert werden, beispielsweise mit Hilfe eines Rechners im Internet. Die Stelle kann auch die mobile Vorrichtung oder ein Ziel-Gerät sein, das automatisch die Übertragung anfordert. Bevorzugt wird vor der Übertragung eine Berechtigungsprüfung für die anfordernde Stelle durchgeführt (Anspruch 8). Hierfür werden Informationen über die Identität der Stelle, welche die Übertragung der Software-Module anfordert, an die Zentrale übermittelt. Beispielsweise werden von einer anfordernden Person eine PIN, ein Paßwort oder ein Fingerabdruck ermittelt und mit abgespeicherten Informationen verglichen. Nur bei erfolgreicher Berechtigungsprüfung werden Software-Module übertragen. Durch die Berechtigungsprüfung wird insbesondere vermieden, dass ein Nutzer sich in den Besitz eines kostenpflichtigen Software-Moduls bringt, ohne dafür bezahlt zu haben, und dass die Übertragung aufgrund eines Fehlers ausgelöst wird.

Um zu verhindern, dass ein Software-Modul beispielsweise bei der Abspeicherung auf der mobilen Speicher-Einrichtung oder der Übertragung verfälscht oder manipuliert oder eine unberechtigt angefertigte Kopie verwendet wurde, wird eine Korrektheitsprüfung durchgeführt (Anspruch 9). Hierzu wird für mindestens ein Software-Modul eine Signatur erzeugt und auf der mobilen Speicher-Einrichtung abgespeichert. Die Signatur wird vorzugsweise dadurch erzeugt, dass das Software-Modul als Datenstrom behandelt wird und ein Hash-Wert erzeugt wird. Mit Hilfe eines geheimen Schlüssels wird aus diesem Hash-Wert

die Signatur erzeugt. Die Signatur hängt also vom Software-Modul und vom geheimen Schlüssel ab.

Weiterhin wird an Bord der mobilen Vorrichtung für mindestens einen Ziel-Geräte-Typ ein öffentlicher Schlüssel abgespeichert. Mit Hilfe dieses öffentlichen Schlüssels wird die Signatur geprüft. Nur bei positivem Ausgang der Prüfung wird das Software-Modul als nicht verfälscht und als berechtigt erkannt.

Eine Übertragungs-Vorrichtung zur Durchführung eines Verfahrens nach einem der Ansprüche 1 bis 9 umfasst gemäß Anspruch 10 eine Einrichtung zur drahtlosen Datenübertragung zwischen Zentrale und mobiler Vorrichtung in beiden Richtungen und eine Steuerungs-Einrichtung, welche die Übermittlung von Software-Modulen von der Zentrale zur mobilen Vorrichtung veranlaßt und steuert. Die Steuerungs-Einrichtung ermittelt die zu Beginn der Übertragung tatsächlich vorhandene Konfiguration der mobilen Vorrichtung, wählt die Menge von Software-Modulen aus, und prüft, welche der ausgewählten Software-Module für die tatsächlich vorhandene Konfiguration freigegeben sind. Weiterhin veranlaßt die Steuerungs-Einrichtung die Übertragung der ausgewählten und freigegebenen Software-Module. Vorzugsweise ermittelt die Steuerungs-Einrichtung, welche Software-Module fehlerfrei an die mobile Vorrichtung übertragen wurden (Anspruch 11).

Bevorzugt reagiert die Steuerungs-Einrichtung auf erkannte Übertragungsfehler. Beispielsweise veranlaßt sie einen zweiten Übertragungs-Versuch, führt eine Fehlerbehandlung durch oder bricht die Übertragung der Software-Module ab.

Im folgenden wird ein Ausführungsbeispiel des erfindungsgemäßen Verfahrens anhand der beiliegenden Zeichnungen näher beschrieben. Dabei zeigen:

Fig. 1. eine beispielhafte Ausführungsform der Erfindung, bei der die Software-Module von einer Zentrale mit Hilfe zweier verschiedener drahtloser Datenübertragungseinrichtungen zur mobilen Vorrichtung übertragen werden;

Fig. 2. eine beispielhafte Systemarchitektur für Zentrale und mobile Vorrichtung.

Im Beispiel der Fig. 1 wird wenigstens zeitweise eine Datenverbindung zwischen der Zentrale 10 und dem ersten Fahrzeug 20.1 und eine weitere Datenverbindung zwischen der Zentrale 10 und dem zweiten Fahrzeug 20.2 hergestellt. Die drahtlosen Datenverbindungen können auf die gleiche oder auf unterschiedliche Weisen hergestellt werden. Als zwei Beispiele sind in Fig. 1 die drahtlose Übertragung mit Hilfe eines Satelliten 50.1 und die über ein Mobilfunknetz 50.2 dargestellt. Die Software-Module werden z. B. über ein Weitverkehrsnetz oder ein lokales Netz übertragen. Die Zentrale kann sich an einem einzigen Ort befinden oder räumlich verteilt sein. Insbesondere falls ein Fahrzeug 20.1 oder 20.2 sich während der Übertragung bewegt, kann die übertragende Zentrale sogar während der Übertragung wechseln.

Bei der Übertragung von Software-Modulen werden für jedes der beiden Fahrzeuge 20.1 und 20.2 die folgenden Verfahrensschritte ausgeführt:

- Insbesondere dann, wenn der Fahrzeug-Hersteller die Software-Module nur dann übermittelt, wenn der Eigentümer der Übertragung der Software-Module zugestimmt hat und / oder die Software-Module bezahlt hat, wird eine Berechtigungsprüfung für die anfordernde Stelle durchgeführt. Hierfür wird beispielsweise ein Fingerabdruck einer anfordernden Person ermittelt oder eine PIN oder ein Paßwort von einer anfordernden Stelle erfaßt und anschließend Fingerabdruck, PIN oder Paßwort an die Zentrale übermittelt und bei einer Berechtigungsprüfung ausgewertet. Nach erfolgreicher Berechtigungsprüfung wird festgestellt, ob der Eigentümer der Übertragung verbindlich zugestimmt hat. Die folgenden Schritte werden nur dann durchgeführt, wenn eine Zustimmung vorliegt oder nicht erforderlich ist.

- Eine eindeutige Kennung des Fahrzeugs, vorzugsweise eine Fahrzeug-Ident-Nummer, wird ermittelt und an die Zentrale übermittelt. Diese Kennung unterscheidet das Fahrzeug von allen anderen Fahrzeugen dieses Herstellers. Zusätzlich werden die Baureihe, das Baumuster und das Baujahr und das Jahr der letzten Änderung übermittelt. Diese Informationen lassen sich zwar oft durch Lesezugriff auf ein zentrales Konfigurations-Management-System ermitteln. Werden sie aber vom Fahrzeug zur Zentrale übermittelt, so wird ein oft zeitraubender Lesezugriff eingespart.
- Die aktuelle Konfiguration des Fahrzeugs wird ermittelt und an die Zentrale übermittelt. Hierbei wird ermittelt, welche Ziel-Geräte vor Beginn der Übertragung an Bord des Fahrzeugs tatsächlich eingebaut sind und welche Software-Module vor Beginn der Übertragung an Bord des Fahrzeugs tatsächlich aktiviert und / oder abgespeichert sind. Vorzugsweise werden Typ-Kennungen für die aktuell eingebauten Geräte und bereits vorhandenen Software-Module, z. B. Sachnummern und Variantenummern, übermittelt. Diese Ermittlung wird bevorzugt dadurch ausgeführt, dass in jedem Ziel-Gerät ein Speicher vorhanden ist, in dem die Konfigurations-Informationen über dieses Ziel-Gerät abgespeichert sind und der z. B. über einen Datenbus angesprochen und ausgelesen wird. Alternative Ausführungsformen bestehen daraus, einen zentralen Speicher an Bord des Fahrzeugs oder Speicherchips, die an den Ziel-Geräten angebracht sind, auszulesen. Insbesondere dann, wenn ein Speicher in einem Ziel-Gerät aufgrund eines Defekts nicht ausgelesen werden kann oder wenn der Speicher eines neuen Ziel-Geräts noch nicht gefüllt ist, besteht ein Notbehelf darin, Markierungen an Geräten, z. B. Strichcodes, optisch zu erfassen.
- Bei Bedarf werden die Informationen über die aktuelle Konfiguration mit einem Datensatz über die Konfiguration des Fahrzeugs verglichen, der in einem Konfigurations-Management-System abgespeichert ist. Dies wird beispielsweise dann durchgeführt, wenn die übermittelten Informationen über die aktuelle Konfiguration lückenhaft oder erkenn-

bar fehlerhaft sind. Zur Erkennung von derartigen Fehlern wird bevorzugt eine Plausibilitätsprüfung der vom Fahrzeug übermittelten und der abgespeicherten Informationen über die Konfiguration durchgeführt.

- Ausgewählt wird eine Menge von Software-Modulen, die von der Zentrale zum Fahrzeug übertragen werden. Die Auswahl hängt von der aktuellen Konfiguration des Fahrzeugs, vom Anwendungsfall und von der Kundenanforderung ab.
- Nur diejenigen Software-Module werden übertragen, die für die aktuelle Konfiguration des Fahrzeugs freigegeben sind. Für jedes Software-Modul wird eine Freigabe-Prüfung durchgeführt, indem Freigabe-Festlegungen ausgewertet werden. Diese Freigabe-Festlegungen umfassen Typ-Kennungen für Ziel-Geräte und Software-Module. Eine Ausführungsform wird weiter unten beschrieben. Mögliche Ergebnisse der Freigabe-Prüfung sind, dass alle, einige oder gar keines der ausgewählten Software-Module als freigegeben erkannt werden.
- Überprüft wird, ob die ausgewählten Software-Module jetzt übertragen werden können. Hierbei wird festgestellt, ob mit Hilfe der drahtlosen Datenübertragungseinrichtung überhaupt eine Verbindung zwischen Zentrale und Fahrzeug vorhanden ist oder aufgebaut werden kann und ob der Übertragungskanal eine für die Übertragung ausreichende Güte, insbesondere eine ausreichende Bandbreite besitzt. Diese Güte kann von dem sende- und Empfangsgerät 190 an Bord des Fahrzeugs abhängen. Beispielsweise wird eine untere Schranke für die Bandbreite oder eine obere Schranke für den Zeitraum, den die Übertragung in Anspruch nimmt, vorgegeben und mit der tatsächlich verfügbaren Bandbreite verglichen. Aus der tatsächlich verfügbaren Bandbreite und der Gesamtgröße der ausgewählten Software-Module wird bei Bedarf ein Wert für den Zeitbedarf der Übertragung vorhergesagt.
- Die ausgewählten und für die aktuelle Konfiguration freigegebenen Software-Module werden komprimiert, so dass die komprimierten Software-Module weniger Speicherplatz als die nicht komprimierten einnehmen. Bekannt sind verschiedene Verfahren zum Komprimieren von Daten.

- Die ausgewählten und für die aktuelle Konfiguration freigegebenen Software-Module werden für die Übertragung konvertiert. Bei Bedarf werden die Software-Module in Teile aufgeteilt. Gemeinsam mit jedem Software-Modul oder Software-Modul-Teil werden Meta-Informationen übertragen, die die Verteilung und Übertragung der Software-Module an Bord sowie deren Aktivierung steuern. Zu diesen Meta-Informationen zählen Parameter, die das verwendete On-Board-Übertragungsprotokoll benötigt.
- Die ausgewählten und für die aktuelle Konfiguration freigegebenen Software-Module werden von der Zentrale zum Fahrzeug übertragen. Als Übertragungstechnik wird beispielsweise ein Mobilfunk-Standard, z. B. GSM oder UMTS, eingesetzt. Vorzugsweise wird ein zur gewählten Übertragungstechnik passendes Protokoll, z. B. das dateibasierte Protokoll zModem, verwendet. Dadurch wird insbesondere nach einem Abbruch der Verbindung eine sichere Fehlerbehandlung mit Synchronisation erleichtert, die weiter unten beschrieben wird.
- Vorzugsweise werden die übertragenen Software-Module an Bord des Fahrzeugs in einem Pufferspeicher abgespeichert.
- Festgestellt wird, welche Software-Module fehlerfrei übertragen wurden. Diese Information wird an die Zentrale übermittelt. Beispielsweise wird nach jeder erfolgreichen Übertragung eines Software-Moduls eine Rückmeldung an die Zentrale übermittelt, oder nach erfolgreicher Übertragung aller Software-Module wird diese Information an die Zentrale übermittelt. Für die Feststellung wird vorzugsweise für jedes Software-Modul oder jedes Software-Modul-Teil eine Soll-Prüfsumme nach dem CRC-Verfahren ermittelt und übertragen. Nach der Übertragung wird an Bord der mobilen Vorrichtung eine Ist-Prüfsumme ermittelt und mit der Soll-Prüfsumme verglichen.
- Vorzugsweise werden Verschlüsselungs-Informationen gemeinsam mit den Software-Modulen übertragen, um zu prüfen, ob die Software-Module aus einer vertrauenswürdigen Quelle stammen und unverfälscht übertragen wurden. Beispielsweise

wird ein Software-Modul in der Zentrale verschlüsselt und an Bord der mobilen Vorrichtung wieder entschlüsselt. Ein Verfahren hierfür ist aus DE 195 32 067 C1 bekannt. Oder ein Software-Modul wird unverschlüsselt, aber gemeinsam mit einer Signatur übertragen. Die Signatur wird mit Hilfe eines geheimen Schlüssels in der Zentrale erzeugt und mit einem öffentlichen Schlüssel verglichen, der beispielsweise zuvor auf einem anderen Kanal zur mobilen Vorrichtung übermittelt wurde.

- Falls festgestellt wurde, dass ein Software-Modul nur fehlerhaft, verfälscht oder gar nicht übertragen wurde, so wird ein zweiter Versuch der Übertragung durchgeführt. Falls zwischen erstem und zweiten Versuch eine größere Zeitspanne verstrichen ist, wird erneut die aktuelle Konfiguration des Fahrzeugs ermittelt, denn diese kann in der Zwischenzeit verändert worden sein. Scheitert auch der zweite Versuch, so wird die unten beschriebene Fehlerbehandlung durchgeführt.
- Daten über den aktuellen Betriebszustand des Fahrzeugs werden erfaßt und an die Zentrale übermittelt. Diese Daten umfassen beispielsweise die aktuelle Fahrgeschwindigkeit, den Motorzustand, den Ladezustand der Batterie und die aktuelle Position des Fahrzeugs. Aufgrund des Betriebszustands wird entschieden, ob die übertragenen Software-Module jetzt aktiviert werden. Dabei wird insbesondere geprüft, ob das Fahrzeug sich in einem sicheren Zustand befindet. Beispielsweise wird der Ladezustand der Batterie berücksichtigt, um sicherzustellen, dass während der gesamten Aktivierung genügend elektrische Spannung zur Verfügung steht. Die aktuelle Position wird beispielsweise ausgewertet, um zu prüfen, in welchem Land oder z. B. US-Bundesstaat sich das Fahrzeug befindet, um bei Bedarf zu prüfen, ob länderspezifische gesetzliche oder technische Randbedingungen zu beachten sind. Bei Bedarf wird der Fahrer des Fahrzeugs gebeten, das Fahrzeug in einen sicheren Zustand zu bringen, z. B. es anzuhalten, und dies zu bestätigen. Dies wird z. B. durch Sprachausgabe und -eingabe oder dadurch durch-

geführt, dass Meldungen angezeigt werden und der Fahrer gebeten wird, diese zu bestätigen.

- Falls alle Software-Module fehlerfrei und unverfälscht übertragen wurden oder der Pufferspeicher vollständig gefüllt ist und falls das Fahrzeug sich in einem sicheren Zustand befindet, werden die übertragenen Software-Module aus dem Pufferspeicher in die Ziel-Geräte übertragen, vorzugsweise über einen Datenbus an Bord des Fahrzeugs. Bei Bedarf werden sie zuvor dekomprimiert. Für diesen Vorgang werden die Meta-Informationen ausgewählt. Nach der Übertragung zu den Geräten werden die Geräte bei Bedarf deaktiviert, die Software-Module aktiviert und danach die Geräte wieder aktiviert.
- In der Zentrale, z. B. in einem Konfigurations-Management-System, wird die aktuelle Konfiguration der mobilen Vorrichtung nach der Übertragung abgespeichert. Die aktuelle Konfiguration umfaßt die Informationen, welche der Ziel-Geräte an Bord tatsächlich eingebaut sind und welche Software-Module entweder fehlerfrei übertragen und aktiviert wurden oder bereits vor der Übertragung aktiviert und durch die Übertragung nicht verändert wurden.
- Ein Konfigurations-Management-System in der Zentrale umfaßt einen Datensatz für das Fahrzeug. Dieser Datensatz wird nach der Übertragung aktualisiert, so dass er nach der Aktualisierung Informationen darüber enthält, welche der Ziel-Geräte an Bord tatsächlich eingebaut sind und welche Software-Module nunmehr aktiviert sind.
- Eine Fehlerbehandlung ist insbesondere dann erforderlich, wenn eine vorgegebene Anzahl von Versuchen Versuche scheitern, alle Software-Module fehlerfrei zu übertragen, beispielsweise weil keine Verbindung zwischen Zentrale und Fahrzeug hergestellt werden kann. Bevorzugt wird bei einer Fehlerbehandlung eine Synchronisation durchgeführt. Hierbei wird festgestellt, welche Software-Module fehlerfrei übertragen wurden. Der Datensatz für das Fahrzeug im zentralen Konfigurations-Management-System wird aktualisiert, und ein Fehlerprotokoll wird generiert. Zu einem späteren Zeitpunkt

wird ein erneuter Übertragungsversuch begonnen, der von einem definierten Zustand ausgeht.

Fig. 2 zeigt eine beispielhafte Systemarchitektur für die Zentrale 10 und das Fahrzeug 20. Die Zentrale 10 umfaßt die folgenden Komponenten:

- ein Central Remote Flashing Manager 160, der die Übermittlung von Software-Modulen von der Zentrale zur mobilen Vorrichtung veranlaßt und steuert und dabei Software-Module auswählt und prüft, ob sie für die aktuelle Konfiguration freigegeben sind,
- eine Steuerungs- und Regelungs-Einrichtung 110, mit dem die erforderlichen Maßnahmen zum Übertragen von Software-Modulen erfaßt und aufgelistet und veranlaßt werden und durch das die Durchführung der Maßnahmen überwacht wird,
- ein Logistiksystem 130, das die benötigten Software-Module identifiziert, auswählt und für die Übertragung bereitstellt,
- ein Abrechnungs-System 140, das die Übertragungsvorgänge kaufmännisch abwickelt und dabei insbesondere die Rechnungslegung durchführt und die Zahlungsvorgänge überwacht,
- ein Informationssystem 150, das den Eigentümer und / oder Fahrer des Fahrzeugs vor der Übertragung über angebotene und durch Software-Module realisierbare funktionale Erweiterungen und Änderungen durch Software-Module und nach der Übertragung über die erfolgreiche Übertragung oder über aufgetretene Fehler informiert und das beispielsweise das Internet verwendet oder die Versendung von Briefen auslöst,
- ein Entscheidungsunterstützungs-System 170, mit dessen Hilfe Software-Module in Abhängigkeit von der aktuellen Fahrzeug-Konfiguration und der durchzuführenden Kundendienst-Maßnahme ausgewählt werden,
- eine Sende- und Empfangseinrichtung 180 in der Zentrale (10) und
- eine Sende- und Empfangseinrichtung 190, die mit dem Fahrzeug 20.1, 20.2 verbunden ist.

Die Sende- und Empfangseinrichtungen 180 und 190 sind beispielsweise als Knoten eines Mobilfunknetzes, das z. B. mit den Übertragungsverfahren GSM oder UMTS arbeiten, oder für eine Übertragung mittels Satelliten ausgebildet. An Bord eines Fahrzeugs können mehrere Sende- und Empfangseinrichtungen 190 eingebaut sein.

Im folgenden wird an einem Ausführungsbeispiel beschrieben, wie die Freigabe-Prüfung durchgeführt wird und welche Freigabe-Festlegungen hierfür ausgewertet werden. In dem Ausführungsbeispiel werden zwei Ziel-Geräte an Bord eines Kraftfahrzeugs 20.1, 20.2 mit Software-Modulen versorgt: eine Zentraleinheit eines Systems zur Sprachausgabe, die z. B. Meldungen an den Fahrer in natürlicher Sprache vorliest, und ein Steuergerät für das Türsystem. Die Zentraleinheit ist mit einem Sende- und Empfangsgerät für drahtlose Datenübertragung und über einen Datenbus mit dem Steuergerät verbunden.

Die beiden Ziel-Geräte stammen von unterschiedlichen Herstellern und werden in verschiedenen Varianten in Fahrzeuge eingebaut. Die Sprachausgabe soll in mehreren Sprachen möglich sein. Die Software-Module für alle Varianten der beiden Ziel-Geräte werden erzeugt und in der Zentrale abgespeichert.

Der Typ eines Ziel-Geräts und der eines Software-Moduls werden durch jeweils eine Sachnummer und eine Variantenummer gekennzeichnet. Die Sachnummer ist eine Abfolge von Ziffern und Buchstaben, die innerhalb des Produktspektrums des Fahrzeug-Herstellers eindeutig ist. Die Variante wird durch eine Zahl mit drei Ziffern gekennzeichnet.

Die Freigabe-Festlegungen sind beispielsweise in einer relationalen Datenbank in Form von Datensätzen in der Zentrale abgespeichert. Für eine Freigabe-Prüfung wird diese Datenbank eingelesen und ausgewertet. Ein Prinzip ist, dass ein Software-Modul nur dann für einen Typ von Ziel-Geräten freigegeben ist, wenn eine entsprechende Freigabe-Festlegung in der Freigabe-Datenbank vermerkt ist, ansonsten nicht.

Jeder Freigabe-Datensatz umfaßt folgende Datenfelder:

- Baureihe,

- Region,
- Ziel-Geräte-Typen,
- Zulieferer,
- Beschreibung_Hardware,
- Art_der_Software,
- Software-Module,
- Beschreibung_Software,
- gültig_ab,
- Voraussetzung.

Mit „Baureihe“ ist die Baureihe des Fahrzeugs gemeint, auf das sich der Freigabe-Datensatz bezieht, z. B. W212. In den Datenfeldern „Ziel-Geräte-Typ“ und „Software-Module“ werden Geräte- bzw. Software-Typ-Kennungen aufgeführt, was im folgenden beispielhaft erläutert wird. Der in dem Datenfeld „gültig_ab“ eingetragene Zeitpunkt legt für den Datensatz den Beginn des Freigabe-Zeitraums fest. Die im Datensatz genannten Software-Module sind nur dann für die genannten Ziel-Geräte-Typen freigegeben, wenn der Zeitpunkt der Übertragung nach dem durch das Datenfeld „gültig_ab“ festgelegten Zeitpunkt liegt. Die Freigabe kann an eine Freigabe-Bedingung gebunden sein, die vorzugsweise als Boole'scher Ausdruck formuliert wird. Die Inhalte der Datenfelder „Beschreibung_Hardware“ und „Beschreibung_Software“ werden nicht automatisch ausgewertet. Sie erläutern vielmehr einem Bearbeiter die Typ-Kennungen.

In dem folgenden Beispiel stammt die Software für die Zentraleinheit vom Zulieferer XY, die für das Tür-Steuergerät von den Zulieferern AB (für den europäischen Markt) und FG (für den US-amerikanischen Markt). Typen von Ziel-Geräten und Software-Module werden durch Sachnummern gekennzeichnet, die mit HW bzw. SW beginnen, gefolgt von drei oder vier Ziffern. Varianten sind durch drei Ziffern gekennzeichnet. SW-212-001 bezeichnet z. B. ein Software-Modul mit der Sachnummer SW-212 und der Variantenummer 001. Typ-Kennungen, zusammengesetzt

aus Sachnummern und Variantennummern, sind in eckige Klammern [] gesetzt.

1. Datensatz

<i>Datenfeld</i>	<i>Inhalt</i>
Baureihe	W212
Region	EUR
Ziel-Geräte-Typen	[HW-1001-001] [HW-1001-002]
Zulieferer	XY
Beschreibung Hardware	Zentraleinheit für Europa
Art der Software	OS
Software-Module	[SW-101-001]
Beschreibung Software	Betriebssystem für Zentraleinheit, V1
gültig ab	1.1.1999
Freigabe-Bedingung	

Das Software-Modul [SW-101-001] ist durch den 1. Datensatz für die Ziel-Geräte-Typen [HW-1001-001] und [HW-1001-002] in Europa freigegeben.

2. Datensatz

<i>Datenfeld</i>	<i>Inhalt</i>
Baureihe	W212
Region	EUR
Ziel-Geräte-Typen	[HW-1001-001] [HW-1001-002]
Zulieferer	XY
Beschreibung Hardware	Zentraleinheit für Europa
Art der Software	APPL
Software-Module	[SW-111-001]
Beschreibung Software	Anwendung für Zentraleinheit, V1

gültig ab	1.3.1999
Freigabe-Bedingung	

Das Software-Modul [SW-111-001] ist durch den 2. Datensatz für die Ziel-Geräte-Typen [HW-1001-001] und [HW-1001-002] in Europa freigegeben.

3. Datensatz

<i>Datenfeld</i>	<i>Inhalt</i>
Baureihe	W212
Region	USA
Ziel-Geräte-Typen	[HW-1002-001] [HW-1002-002]
Zulieferer	XY
Beschreibung Hardware	Zentraleinheit für USA
Art der Software	OS
Software-Module	[SW-102-001]
Beschreibung Software	Betriebssystem für Zentraleinheit, V1
gültig ab	1.4.1999
Freigabe-Bedingung	

Das Software-Modul [SW-102-001] ist durch den 3. Datensatz für die Ziel-Geräte-Typen [HW-1002-001] und [HW-1002-002] in den USA freigegeben.

4. Datensatz

<i>Datenfeld</i>	<i>Inhalt</i>
Baureihe	W212
Region	USA
Ziel-Geräte-Typen	[HW-1002-001] [HW-1002-002]
Zulieferer	XY
Beschreibung Hardware	Zentraleinheit für USA

Art der Software	APPL
Software-Module	[SW-112-001]
Beschreibung Software	Anwendung für Zentraleinheit, V1
gültig ab	1.4.1999
Freigabe-Bedingung	[HW-1102-00n] AND ([HW-2102-001] OR [HW-2102-002]) AND NOT [HW-2302-00n]

Das Software-Modul [SW-112-001] ist durch den 4. Datensatz für die Ziel-Geräte-Typen [HW-1002-001] und [HW-1002-002] in den USA freigegeben, falls die Freigabe-Bedingung erfüllt ist. Die Freigabe-Bedingung ist erfüllt, wenn

- ein Ziel-Gerät vom Typ HW-1102 und einer der Varianten 001 bis 009
- und ein Ziel-Gerät vom Typ HW-2102 und der Variante 001 oder 002
- und kein Ziel-Gerät vom Typ HW-2302, das von einer der Varianten 001 bis 009 ist,

eingebaut ist. Hierbei ist 00n eine abkürzende Bezeichnung für die Varianten 001 bis 009.

5. Datensatz

<i>Datenfeld</i>	<i>Inhalt</i>
Baureihe	W212
Region	EUR
Ziel-Geräte-Typen	[HW-2001-001] [HW-2001-002]
Zulieferer	AB
Beschreibung Hardware	Tür-Steuergerät für Europa
Art der Software	TOOL
Software-Module	[SW-221-001]
Beschreibung Software	Diagnose für Tür-Steuergerät, V1
gültig ab	1.5.1999

Freigabe-Bedingung	[HW-2002-001] OR [HW-2302-00n]
--------------------	--------------------------------

Das Software-Modul [SW-221-001] ist durch den 5. Datensatz für die Ziel-Geräte-Typen [HW-2001-001] und [HW-2001-002] in Europa freigegeben, falls die Freigabe-Bedingung erfüllt ist. Die Freigabe-Bedingung ist erfüllt, wenn an Bord

- ein Ziel-Gerät vom Typ [HW-2002-001]
 - oder ein Ziel-Gerät vom Typ HW-2302, das von einer der Varianten 001 bis 009 ist,
- eingebaut ist.

6. Datensatz

<i>Datenfeld</i>	<i>Inhalt</i>
Baureihe	W212
Region	USA
Ziel-Geräte-Typen	[HW-2002-001] [HW-2002-002]
Zulieferer	FG
Beschreibung Hardware	Tür-Steuergerät für USA
Art der Software	TOOL
Software-Module	[SW-222-001]
Beschreibung Software	Diagnose für Tür-Steuergerät, V1
gültig ab	1.6.1999
Freigabe-Bedingung	[SW-221-001]

Das Software-Modul [SW-111-001] ist durch den 6. Datensatz für die Ziel-Geräte-Typen [HW-1001-001] und [HW-1001-002] in den USA freigegeben, falls an Bord das Software-Modul [SW-221-001] aktiviert ist.

Bei der Auswertung der Freigabe-Datei wird für jedes Ziel-Gerät, das im Fahrzeug vorkommt, die Freigabe-Datenbank durchsucht. Für jeden Datensatz wird das Datenfeld „Baureihe“ abgeglichen und das Datenfeld „Ziel-Geräte-Typen“ ausgewer-

tet. Ist an Bord ein Ziel-Gerät eines er im Datenfeld „Ziel-Geräte-Typen“ genannten Typen eingebaut, so wird festgestellt, ob eine Freigabe-Bedingung formuliert ist. Ist dies der Fall, so wird geprüft, ob die Freigabe-Bedingung auf Erfüllungsein geprüft. Ist die Freigabe-Bedingung erfüllt oder ist keine Freigabe-Bedingung formuliert, so sind alle Software-Module für das Fahrzeug freigegeben, die im Datenfeld „Software-Module“ des Datensatzes genannt sind. Welche der freigegebenen Software-Module tatsächlich übertragen werden, hängt davon ab, welche Software-Module ausgewählt worden sind.

Für jedes Software-Modul werden weiterhin Konfigurations- und Sicherheits-Informationen beispielsweise in zwei Datenbanken für Software-Module und zwei für Software-Modul-Teile erzeugt, in der Zentrale abgespeichert und bei der Übertragung ausgewertet. Die eine Datenbank ist die Konfigurations-Datenbank, die andere die Sicherheits-Datenbank.

Die Informationen in der Konfigurations-Datenbank legen fest, welche Dateien zum Software-Modul gehören, wo diese Dateien abgespeichert sind und in welcher Reihenfolge sie wohin, d. h. zu welchem Ziel-Gerät, übertragen werden. Mit Hilfe der Sicherheits-Informationen werden Übertragungsfehler und Manipulationen erkannt.

Ein Datensatz für ein Software-Modul in der Konfigurations-Datenbank für Software-Module umfaßt beispielsweise folgende Datenfelder:

- Software-Modul,
- Ziel-Adresse,
- Größe,
- Speicherort,
- Prüfverfahren,
- Prüfsumme,
- Teile_Kennungen.

Das Datenfeld „Ziel-Adresse“ gibt die Ziel-Adresse des Ziel-Geräts auf dem Datenbus im Fahrzeug an, z. B. #57 für das Tür-Steuergerät und #20 für die Zentraleinheit.

Das Datenfeld „Größe“ gibt die Größe des Software-Moduls in KByte an. Diese Angabe wird z. B. für eine Fortschrittsanzeige beim Übertragen verwendet. Festgestellt wird, wie viele KByte bereits übertragen sind, und durch die Angabe in der Konfigurations-Datei ist bekannt, wie viele KByte insgesamt zu übertragen sind. Der Quotient gibt den Arbeitsfortschritt an, der z. B. als Balken angezeigt wird.

Das Datenfeld „Speicherort“ gibt an, wo dieses Software-Modul in der Zentrale abgespeichert ist, beispielsweise in Form eines Pfades eines Betriebssystems oder einer Zugriffsinformation auf eine Datenbank.

Das Datenfeld „Teile_Kennungen“ ist nur dann ausgefüllt, wenn das Software-Modul nicht auf einmal, sondern in mehreren Teilen übertragen wird.

Beispielsweise umfaßt der Datensatz für das Software-Modul [SW-111-001] in der Konfigurations-Datenbank folgende Einträge:

7. Datensatz

<i>Datenfeld</i>	<i>Inhalt</i>
Software-Modul	[SW-111-001]
Ziel-Adresse	#20
Größe	256
Speicherort	/XY/EUR/APPL/V1
Prüfverfahren	CRC
Prüfsumme	4758A08C
Teile_Kennungen	

Durch den 7. Datensatz wird festgelegt, dass die Übertragung des Software-Moduls [SW-111-001] mit dem CRC-Verfahren ge-

prüft wird. Durch die Prüfung wird festgestellt, ob bei der Übermittlung zum Fahrzeug und der Speicherung an Bord des Fahrzeugs ein Übertragungsfehler aufgetreten ist. Als Prüfsumme wird ein CRC-Wert, in diesem Beispiel die Hexadezimalzahl 4758A08C, angegeben. Das Software-Modul wird auf einmal übertragen, daher ist das Datenfeld „Teile_Kennungen“ leer.

Falls ein Software-Modul in mehreren Teilen übertragen wird, so werden jedem Software-Modul-Teil ein eigenes Prüfverfahren und eine eigene Prüfsumme zugewiesen.

Für jedes der Software-Modul-Teile wird in der Konfigurations-Datenbank für Teile ein eigener Datensatz mit folgenden Feldern angelegt:

- Teile-Kennung,
- Größe,
- Speicherort,
- Prüfverfahren,
- Prüfsumme.

Das Datenfeld „Speicherort“ gibt an, wo dieser Software-Modul-Teil in der Zentrale abgespeichert ist.

Ein Datensatz in der Sicherheits-Datenbank umfaßt folgende Datenfelder:

- Software-Modul,
- Ziel-Geräte-Typ,
- Signatur.

8. Datensatz

<i>Datenfeld</i>	<i>Inhalt</i>
Software-Modul	[SW-111-001]
Ziel-Geräte-Typ	[HW-1001-001]
Signatur	85A47D238

9. Datensatz

<i>Datenfeld</i>	<i>Inhalt</i>
Software-Modul	[SW-111-001]
Ziel-Geräte-Typ	[HW-1001-002]
Signatur	9CA47D236

Das Software-Modul [SW-111-001] ist in diesem Beispiel für zwei Varianten von Ziel-Geräten freigegeben, nämlich für die Varianten 001 und 002 des Typs HW-1001. Daher werden zwei verschiedene Signaturen erzeugt und in dem 8. und 9. Datensatz abgespeichert, nämlich eine Signatur pro Variante des Ziel-Geräte-Typs. Die Signatur für eine Variante wird vorzugsweise dadurch erzeugt, dass die Variante als Datenstrom behandelt wird und ein Hash-Wert erzeugt wird. Mit Hilfe eines geheimen Schlüssels wird aus diesem Hash-Wert die Signatur erzeugt. Die Signatur hängt also vom Software-Modul und vom geheimen Schlüssel ab. Für die Erzeugung der Signatur wird beispielsweise eine 1024-Bit-Verschlüsselung nach dem Algorithmus von Rivest-Shamir-Adleman (RSA-Verschlüsselung) verwendet.

Die Erzeugung von Signaturen wird auf einem Rechner durchgeführt, der streng gegen unberechtigten Zugriff und gegen Manipulationen geschützt wird. Beispielsweise betreibt der Zulieferer diesen Rechner und liefert die beiden Varianten und die beiden Signaturen an den Hersteller des Kraftfahrzeuges. Eine andere Ausführungsform ist die, dass der Zulieferer lediglich die beiden Varianten an den Hersteller liefert und dieser selber die Signaturen erzeugt. Beispielsweise übermittelt der Hersteller die Signaturen an den Zulieferer, und dieser überträgt die Software-Module auf seine Ziel-Geräte und verwendet dabei die Signatur für eine Prüfung. Eine dritte Ausführungsform besteht daraus, dass ein zertifiziertes Trust Center die Signaturen erzeugt und die geheimen Schlüssel verwaltet.

In einem permanenten, nicht überschreibbaren Speicher des Ziel-Geräts wird ein öffentlicher Schlüssel abgespeichert. Der öffentliche Schlüssel kann ausgelesen werden, er ist aber sowohl vor versehentlichem als auch vor vorsätzlichem Überschreiben oder Verfälschen oder Löschen geschützt. Vorzugsweise versieht der Zulieferer das Ziel-Gerät mit dem öffentlichen Schlüssel. Die Signatur wird nach dem Übertragen und vor dem Aktivieren des Software-Moduls mit Hilfe des öffentlichen Schlüssels geprüft. Durch diese Prüfung wird sichergestellt, dass das Software-Modul von einer vertrauenswürdigen Quelle kommt und nicht verfälscht oder manipuliert wurde.

Als On-Board-Übertragungsprotokoll wird beispielsweise das „Keyword Protocol 2000“ (KWP2000) verwendet, das durch ISO 14230-1 und ISO 15765-1 bis 15765-4 und VDA 14230-1 bis VDA 14230-3 standardisiert wird. Befehle werden in KWP2000 durch Hexadezimal-Zahlen codiert, z.B. der Befehl „ReadEUIDentification“ (Auslesen einer Typ-Kennung für ein Ziel-Gerät) durch \$1A,86. Die mit einem Software-Modul übertragenen Meta-Informationen umfassen die für das Protokoll KWP2000 notwendigen Kommunikations-Parameter, die die Übertragung an Bord vom Pufferspeicher an ein Ziel-Gerät steuern, z. B. Blockgrößen, Timing-Parameter, Ablaufinformationen und Adresse des Geräts auf dem Datenbus. Andere Übertragungsprotokolle sind ebenfalls geeignet. Die Meta-Informationen werden beispielsweise ebenfalls in Form einer Tabelle übertragen. Diese Tabelle wird im Gegensatz zu der Tabelle für die Freigabe-Prüfung erst während des Übertragungsvorganges generiert.

Nachdem festgestellt wird, dass die ausgewählten und als freigegeben erkannten Software-Module fehlerfrei und unverfälscht übertragen wurden, werden mindestens folgende Informationen an die Zentrale übermittelt:

- eine eindeutige Kennung des Fahrzeugs,
- welche Software-Module fehlerfrei und unverfälscht übertragen wurden,
- welches Gerät, z. B. welcher Diagnosetester, für die Übertragung verwendet wurde

- und das Datum und der Zeitpunkt, zu dem die Übertragung abgeschlossen wurde.

Diese Informationen werden in der Zentrale, beispielsweise in einem Konfigurations-Management-System, abgespeichert, und zwar bevorzugt in dem Datensatz für das Fahrzeug. Dort wird weiterhin abgespeichert, wer die Übermittlung veranlaßt hat.

Bezugszeichenliste

Zeichen	Bedeutung
10	Zentrale
20.1, 20.2	mobile Vorrichtungen mit Ziel-Geräten
50	Einrichtung zur drahtlosen Übertragung
110	Steuerungs- und Regelungs-Einrichtung
130	Logistiksystem
140	Abrechnungs-System
150	Informationssystem
160	Central Remote Flashing Manager
170	Entscheidungsunterstützungs-System
180	Sende- und Empfangseinrichtung in der Zentrale
190	Mit dem Fahrzeug verbundene Sende- und Empfangseinrichtung

Patentansprüche

1. Verfahren zum Übertragen von Software-Modulen von einer Zentrale (10) zu einer Ziel-Vorrichtung (20.1, 20.2) mit Hilfe einer Einrichtung zur Datenübertragung in beiden Richtungen, wobei
 - an Bord der Ziel-Vorrichtung (20.1, 20.2) Ziel-Geräte vorhanden sind,
 - für die Ziel-Geräte Geräte-Typ-Kennungen festgelegt werden,
 - für die Software-Module Software-Typ-Kennungen festgelegt werden,
 - Informationen über die Konfiguration der Ziel-Vorrichtung (20.1, 20.2) an die Zentrale (10) übermittelt werden
 - und eine Menge von Software-Modulen ausgewählt wird, dadurch gekennzeichnet, dass
 - die Datenübertragungseinrichtung eine drahtlose ist,
 - die Ziel-Vorrichtung (20.1, 20.2) eine mobile Vorrichtung, insbesondere ein Verkehrs- oder Transportmittel, ist,
 - die Informationen über die Konfiguration eine Auflistung umfassen, welche Ziel-Geräte und welche Software-Module zu Beginn der Übertragung an Bord der Ziel-Vorrichtung (20.1, 20.2) tatsächlich vorhanden sind,

- Freigabe-Festlegungen vorgegeben sind, die unter Verwendung der Geräte-Typ-Kennungen und Software-Typ-Kennungen festlegen, welche Software-Module für welche Ziel-Geräte-Typen freigegeben sind,
- unter Verwendung der Freigabe-Festlegungen geprüft wird, welche der ausgewählten Software-Module für die tatsächlich vorhandene Konfiguration freigegeben sind
- und die für die Konfiguration freigegebenen Software-Module übertragen werden.

2. Verfahren nach Anspruch 1,
d a d u r c h g e k e n n z e i c h n e t ,
dass bei der Auswahl der Menge von Software-Modulen
die tatsächlich vorhandene Konfiguration der mobilen Vorrichtung (20.1, 20.2) mit einer Soll-Konfiguration verglichen wird
und die Software-Module in Abhängigkeit von der Abweichung zwischen der tatsächlich vorhandenen und der Soll-Konfiguration ausgewählt werden.
3. Verfahren nach Anspruch 1 oder Anspruch 2,
d a d u r c h g e k e n n z e i c h n e t ,
dass vor der Übertragung der Software-Module geprüft wird,
ob mit Hilfe der drahtlosen Datenübertragungseinrichtung ein Übertragungskanal mit einer für die Übertragung ausreichenden Güte aufgebaut werden kann.
4. Verfahren nach einem der Ansprüche 1 bis 3,
d a d u r c h g e k e n n z e i c h n e t ,
dass
 - Informationen über eine der Zentrale bekannten Konfiguration der mobilen Vorrichtung (20.1, 20.2) in einem

Konfigurations-Management-System oder Dokumentations-System abgespeichert werden

- eine Kennung der mobilen Vorrichtung (20.1, 20.2) zur Zentrale (10) übermittelt wird,
- die an die Zentrale (10) übermittelten Informationen über die tatsächlich vorhandene Konfiguration mit denen über die abgespeicherten Konfiguration verglichen werden
- und mindestens eine nicht übermittelte Information über die tatsächlich vorhandene Konfiguration durch Leszugriff auf die abgespeicherte Konfiguration ersetzt oder ergänzt wird.

5. Verfahren nach einem der Ansprüche 1 bis 4,
d a d u r c h g e k e n n z e i c h n e t ,
dass nach der Übertragung mindestens eines der Software-Module die Information an die Zentrale (10) übermittelt werden,

ob das Software-Modul tatsächlich fehlerfrei an die mobile Vorrichtung (20.1, 20.2) übermittelt wurde.

6. Verfahren nach Anspruch 5,
d a d u r c h g e k e n n z e i c h n e t ,
dass
- eine Kennung der mobilen Vorrichtung (20.1, 20.2) zur Zentrale (10) übermittelt wird,
 - und in einem Konfigurations-Management-System die Information abgespeichert wird,

welche Ziel-Geräte und welche Software-Module nach Abschluß der Übertragung an Bord der mobilen Vorrichtung (20.1, 20.2) tatsächlich vorhanden sind.

7. Verfahren nach einem der Ansprüche 1 bis 6,
dadurch gekennzeichnet,
dass
- dass zusätzlich Informationen über den aktuellen Betriebszustand der mobilen Vorrichtung (20.1, 20.2) an die Zentrale (10) übermittelt werden,
 - in Abhängigkeit von den Betriebszustands-Informationen entschieden wird, ob die mobile Vorrichtung (20.1, 20.2) sich in einem sicheren Zustand befindet,
 - und dann, wenn sie sich in einem sicheren Zustand befindet, die übertragenen Software-Module aktiviert werden.
8. Verfahren nach einem der Ansprüche 1 bis 7,
dadurch gekennzeichnet,
dass
- Informationen über die Identität der Stelle, die die Übertragung der Software-Module anfordert, an die Zentrale (10) übermittelt werden
 - und eine Berechtigungsprüfung für die anfordernde Stelle durchgeführt wird.
9. Verfahren nach einem der Ansprüche 1 bis 8,
dadurch gekennzeichnet,
dass
- für mindestens ein Software-Modul mit Hilfe eines geheimen Schlüssels eine Signatur erzeugt wird,
 - an Bord der mobilen Vorrichtung für mindestens ein Ziel-Gerät ein öffentlicher Schlüssel abgespeichert wird
 - und die Signatur mit Hilfe des öffentlichen Schlüssels geprüft wird.

10. Übertragungs-Vorrichtung zur Durchführung des Verfahrens nach einem der Ansprüche 1 bis 9,

folgende Bestandteile umfassend:

- eine Einrichtung zur drahtlosen Datenübertragung zwischen der Zentrale (10) und der mobilen Vorrichtung (20.1, 20.2) in beiden Richtungen
- und eine Steuerungs-Einrichtung zur Veranlassung der Übermittlung von Software-Modulen von der Zentrale (10) zur mobilen Vorrichtung (20.1, 20.2), wobei die Steuerungs-Einrichtung
 - eine Einrichtung zur Ermittlung der zu Beginn der Übertragung tatsächlich vorhandenen Konfiguration der mobilen Vorrichtung (20.1, 20.2),
 - eine Einrichtung (170) zur Auswahl der Menge von Software-Modulen,
 - eine Einrichtung (160) für eine Prüfung, welche Software-Module für die tatsächlich vorhandene Konfiguration freigegeben sind,
 - und eine Einrichtung zur Auswertung der Freigabe-Festlegungen

umfaßt.

11. Übertragungs-Vorrichtung nach Anspruch 10,

d a d u r c h g e k e n n z e i c h n e t ,

dass die Steuerungs-Einrichtung eine Einrichtung zur Ermittlung, welche Software-Module fehlerfrei an die mobile Vorrichtung (20.1, 20.2) übertragen wurden, umfaßt.

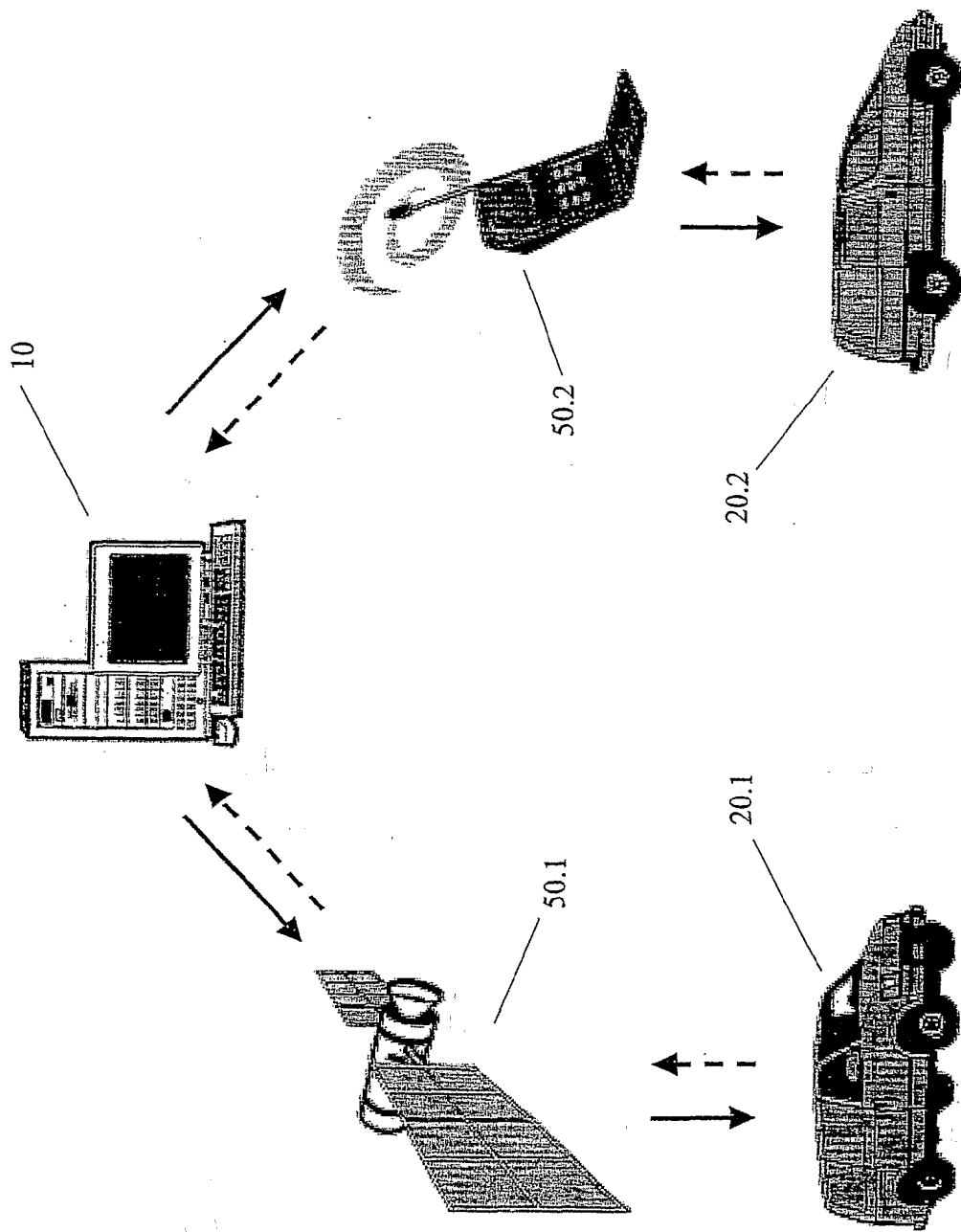
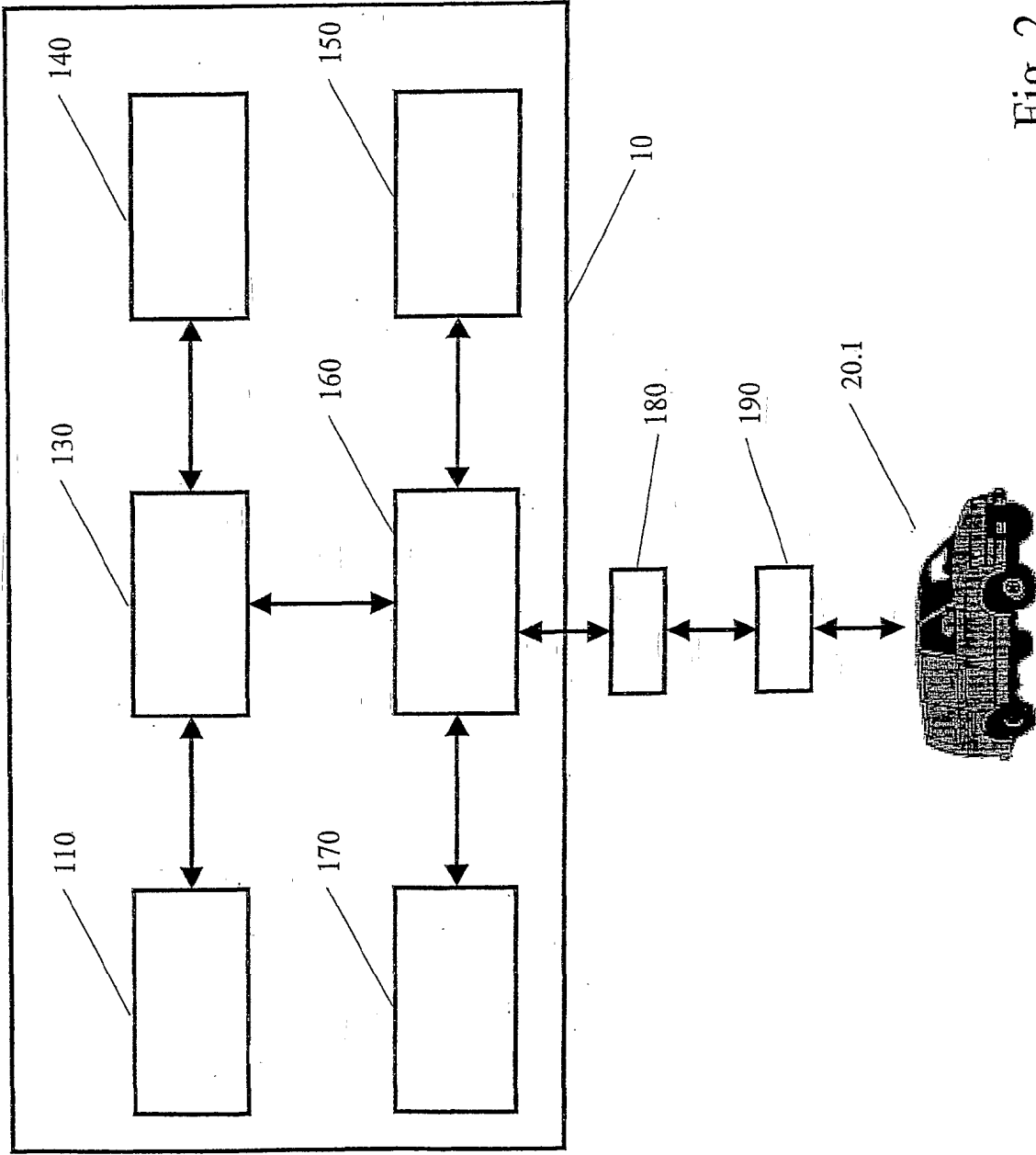


Fig. 1



INTERNATIONAL SEARCH REPORT

International Application No

PCT/EP 02/06994

A. CLASSIFICATION OF SUBJECT MATTER
 IPC 7 G06F9/445 H04Q7/32

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC 7 G06F H04Q

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

EPO-Internal, WPI Data, IBM-TDB

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5 867 714 A (TERRELL MICHAEL R ET AL) 2 February 1999 (1999-02-02) claims 8,14; figure 1 column 4, line 50 column 7-11 column 12, line 15	1-11
A	EP 0 778 520 A (SUN MICROSYSTEMS INC) 11 June 1997 (1997-06-11) abstract; figure 1	9
A	GB 2 352 539 A (HUGH SYMONS GROUP PLC) 31 January 2001 (2001-01-31) abstract; figures 1B,11	1,2

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

* Special categories of cited documents:

- *A* document defining the general state of the art which is not considered to be of particular relevance
- *E* earlier document but published on or after the international filing date
- *L* document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
- *O* document referring to an oral disclosure, use, exhibition or other means
- *P* document published prior to the international filing date but later than the priority date claimed

- *T* later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
- *X* document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
- *Y* document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.
- * & * document member of the same patent family

Date of the actual completion of the international search

19 November 2002

Date of mailing of the international search report

27/11/2002

Name and mailing address of the ISA

European Patent Office, P.B. 5818 Patentlaan 2
 NL - 2280 HV Rijswijk
 Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
 Fax: (+31-70) 340-3016

Authorized officer

Krischer, S

INTERNATIONAL SEARCH REPORT

Information on patent family members

In International Application No

PCT/EP 02/06994

Patent document cited in search report		Publication date	Patent family member(s)	Publication date
US 5867714	A	02-02-1999	NONE	
EP 0778520	A	11-06-1997	US 5692047 A	25-11-1997
			AU 717615 B2	30-03-2000
			AU 7185696 A	12-06-1997
			CA 2190556 A1	09-06-1997
			EP 0778520 A2	11-06-1997
			JP 10011281 A	16-01-1998
			SG 75108 A1	19-09-2000
			US 6070239 A	30-05-2000
GB 2352539	A	31-01-2001	AU 4132900 A	17-11-2000
			EP 1185923 A2	13-03-2002
			WO 0067112 A2	09-11-2000

INTERNATIONALER RECHERCHENBERICHT

Int. Verord. Aktenzeichen

PCT/EP 02/06994

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
 IPK 7 G06F9/445 H04Q7/32

Nach der Internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
 IPK 7 G06F H04Q

Recherchierte aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)

EPO-Internal, WPI Data, IBM-TDB

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X	US 5 867 714 A (TERRELL MICHAEL R ET AL) 2. Februar 1999 (1999-02-02) Ansprüche 8,14; Abbildung 1 Spalte 4, Zeile 50 Spalte 7-11 Spalte 12, Zeile 15	1-11
A	EP 0 778 520 A (SUN MICROSYSTEMS INC) 11. Juni 1997 (1997-06-11) Zusammenfassung; Abbildung 1	9
A	GB 2 352 539 A (HUGH SYMONS GROUP PLC) 31. Januar 2001 (2001-01-31) Zusammenfassung; Abbildungen 1B,11	1,2

☐ Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen

☒ Siehe Anhang Patentfamilie

* Besondere Kategorien von angegebenen Veröffentlichungen :

A Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist

E älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist

L Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)

O Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht

P Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist

T Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist

X Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden

Y Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist

Z Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche

19. November 2002

Absenddatum des internationalen Recherchenberichts

27/11/2002

Name und Postanschrift der Internationalen Recherchenbehörde
 Europäisches Patentamt, P.B. 5818 Patentlaan 2
 NL - 2280 HV Rijswijk
 Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
 Fax: (+31-70) 340-3016

Bevollmächtigter Bediensteter

Krischer, S

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Internationales Aktenzeichen

PCT/EP 02/06994

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
US 5867714	A	02-02-1999	KEINE
EP 0778520	A	11-06-1997	US 5692047 A 25-11-1997
		AU 717615 B2	30-03-2000
		AU 7185696 A	12-06-1997
		CA 2190556 A1	09-06-1997
		EP 0778520 A2	11-06-1997
		JP 10011281 A	16-01-1998
		SG 75108 A1	19-09-2000
		US 6070239 A	30-05-2000
GB 2352539	A	31-01-2001	AU 4132900 A 17-11-2000
		EP 1185923 A2	13-03-2002
		WO 0067112 A2	09-11-2000